(1) *Requirements and concepts.* The RSPP must require a description of the preliminary safety analysis, including:

(i) A complete description of methods used to evaluate a system's behavioral characteristics;

(ii) A complete description of risk assessment procedures;

(iii) The system safety precedence followed; and

(iv) The identification of the safety assessment process.

(2) *Design for verification and validation.* The RSPP must require the identification of verification and validation methods for the preliminary safety analysis, initial development process, and future incremental changes, including standards to be used in the verification and validation process, consistent with appendix C to this part. The RSPP must require that references to any non-published standards be included in the PSP.

(3) *Design for human factors.* The RSPP must require a description of the process used during product development to identify human factors issues and develop design requirements which address those issues.

(4) *Configuration management control plan.* The RSPP must specify requirements for configuration management for all products to which this subpart applies.

(c) *How are RSPP's approved?* (1) Each railroad shall submit a petition for approval of an RSPP to the Associate Administrator for Safety, FRA, 1200 New Jersey Avenue, SE., Mail Stop 25, Washington, DC 20590. The petition must contain a copy of the proposed RSPP, and the name, title, address, and telephone number of the railroad's primary contact person for review of the petition.

(2) Normally within 180 days of receipt of a petition for approval of an RSPP, FRA:

(i) Grants the petition, if FRA finds that the petition complies with applicable requirements of this subpart, attaching any special conditions to the approval of the petition as necessary to carry out the requirements of this subpart;

(ii) Denies the petition, setting forth reasons for denial; or

(iii) Requests additional information.

(3) If no action is taken on the petition within 180 days, the petition remains pending for decision. The petitioner is encouraged to contact FRA for information concerning its status.

(4) FRA may reopen consideration of any previously-approved petition for cause, providing reasons for such action.

(d) *How are RSPP's modified?* (1) Railroads shall obtain FRA approval for any modification to their RSPP which affects a safety-critical requirement of a PSP. Other modifications do not require FRA approval.

(2) Petitions for FRA approval of RSPP modifications are subject to the same procedures as petitions for initial RSPP approval, as specified in paragraph (c) of this section. In addition, such petitions must identify the proposed modification(s) to be made, the reason for the modification(s), and the effect of the modification(s) on safety.

[70 FR 11095, Mar. 7, 2005, as amended at 74 FR 25174, May 27, 2009]

§ 236.907 Product Safety Plan (PSP).

(a) *What must a PSP contain?* The PSP must include the following:

(1) A complete description of the product, including a list of all product components and their physical relationship in the subsystem or system;

(2) A description of the railroad operation or categories of operations on which the product is designed to be used, including train movement density, gross tonnage, passenger train movement density, hazardous materials volume, railroad operating rules, and operating speeds;

(3) An operational concepts document, including a complete description of the product functionality and information flows;

(4) A safety requirements document, including a list with complete descriptions of all functions which the product performs to enhance or preserve safety;

(5) A document describing the manner in which product architecture satisfies safety requirements;

(6) A hazard log consisting of a comprehensive description of all safety-relevant hazards to be addressed during the life cycle of the product, including maximum threshold limits for each hazard (for unidentified hazards, the

threshold shall be exceeded at one occurrence);

(7) A risk assessment, as prescribed in § 236.909 and appendix B to this part;

(8) A hazard mitigation analysis, including a complete and comprehensive description of all hazards to be addressed in the system design and development, mitigation techniques used, and system safety precedence followed, as prescribed by the applicable RSPP;

(9) A complete description of the safety assessment and verification and validation processes applied to the product and the results of these processes, describing how subject areas covered in appendix C to this part are either: addressed directly, addressed using other safety criteria, or not applicable;

(10) A complete description of the safety assurance concepts used in the product design, including an explanation of the design principles and assumptions;

(11) A human factors analysis, including a complete description of all human-machine interfaces, a complete description of all functions performed by humans in connection with the product to enhance or preserve safety, and an analysis in accordance with appendix E to this part or in accordance with other criteria if demonstrated to the satisfaction of the Associate Administrator for Safety to be equally suitable;

(12) A complete description of the specific training of railroad and contractor employees and supervisors necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the product;

(13) A complete description of the specific procedures and test equipment necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the product. These procedures, including calibration requirements, shall be consistent with or explain deviations from the equipment manufacturer's recommendations;

(14) An analysis of the applicability of the requirements of subparts A through G of this part to the product that may no longer apply or are satisfied by the product using an alternative method, and a complete explanation of the manner in which those requirements are otherwise fulfilled (see § 234.275 of this chapter and § 236.901(c));

(15) A complete description of the necessary security measures for the product over its life-cycle;

(16) A complete description of each warning to be placed in the Operations and Maintenance Manual identified in § 236.919, and of all warning labels required to be placed on equipment as necessary to ensure safety;

(17) A complete description of all initial implementation testing procedures necessary to establish that safety-functional requirements are met and safety-critical hazards are appropriately mitigated;

(18) A complete description of:

(i) All post-implementation testing (validation) and monitoring procedures, including the intervals necessary to establish that safety-functional requirements, safety-critical hazard mitigation processes, and safety-critical tolerances are not compromised over time, through use, or after maintenance (repair, replacement, adjustment) is performed; and

(ii) Each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspections, tests, repairs, replacements, adjustments, and the system's resulting conditions, including records of component failures resulting in safety-relevant hazards (see § 236.917(e)(3));

(19) A complete description of any safety-critical assumptions regarding availability of the product, and a complete description of all backup methods of operation; and

(20) A complete description of all incremental and predefined changes (see paragraphs (b) and (c) of this section).

(b) *What requirements apply to predefined changes?* (1) Predefined changes are not considered design modifications requiring an entirely new safety verification process, a revised PSP, and an informational filing or petition for approval in accordance with § 236.915. However, the risk assessment for the product must demonstrate that operation of the product, as modified by any predefined change,

satisfies the minimum performance standard.

(2) The PSP must identify configuration/revision control measures designed to ensure that safety-functional requirements and safety-critical hazard mitigation processes are not compromised as a result of any such change. (Software changes involving safety functional requirements or safety critical hazard mitigation processes for components in use are also addressed in paragraph (c) of this section.)

(c) *What requirements apply to other product changes?* (1) Incremental changes are planned product version changes described in the initial PSP where slightly different specifications are used to allow the gradual enhancement of the product's capabilities. Incremental changes shall require verification and validation to the extent the changes involve safety-critical functions.

(2) Changes classified as maintenance require validation.

(d) *What are the responsibilities of the railroad and product supplier regarding communication of hazards?* (1) The PSP shall specify all contractual arrangements with hardware and software suppliers for immediate notification of any and all safety critical software upgrades, patches, or revisions for their processor-based system, sub-system, or component, and the reasons for such changes from the suppliers, whether or not the railroad has experienced a failure of that safety-critical system, subsystem, or component.

(2) The PSP shall specify the railroad's procedures for action upon notification of a safety-critical upgrade, patch, or revision for this processor-based system, sub-system, or component, and until the upgrade, patch, or revision has been installed; and such action shall be consistent with the criterion set forth in §236.915(d) as if the failure had occurred on that railroad.

(3) The PSP must identify configuration/revision control measures designed to ensure that safety-functional requirements and safety-critical hazard mitigation processes are not compromised as a result of any such change, and that any such change can be audited.

(4) Product suppliers entering into contractual arrangements for product support described in a PSP must promptly report any safety-relevant failures and previously unidentified hazards to each railroad using the product.

§236.909 Minimum performance standard.

(a) *What is the minimum performance standard for products covered by this subpart?* The safety analysis included in the railroad's PSP must establish with a high degree of confidence that introduction of the product will not result in risk that exceeds the previous condition. The railroad shall determine, prior to filing its petition for approval or informational filing, that this standard has been met and shall make available the necessary analyses and documentation as provided in this subpart.

(b) *How does FRA determine whether the PSP requirements for products covered by subpart H have been met?* With respect to any FRA review of a PSP, the Associate Administrator for Safety independently determines whether the railroad's safety case establishes with a high degree of confidence that introduction of the product will not result in risk that exceeds the previous condition. In evaluating the sufficiency of the railroad's case for the product, the Associate Administrator for Safety considers, as applicable, the factors pertinent to evaluation of risk assessments, listed in §236.913(g)(2).

(c) *What is the scope of a full risk assessment required by this section?* A full risk assessment performed under this subpart must address the safety risks affected by the introduction, modification, replacement, or enhancement of a product. This includes risks associated with the previous condition which are no longer present as a result of the change, new risks not present in the previous condition, and risks neither newly created nor eliminated whose nature (probability of occurrence or severity) is nonetheless affected by the change.

(d) *What is an abbreviated risk assessment, and when may it be used?* (1) An abbreviated risk assessment may be used in lieu of a full risk assessment to